

Written Testimony of Prof. Sandra Aistars
Clinical Professor and Senior Scholar and Director of Copyright Research and Policy of
the Center for the Protection of Intellectual Property (CPIP)

Senate Committee on the Judiciary
Subcommittee on Intellectual Property

***The Digital Millennium Copyright Act at 22: What it is, Why it Was Enacted, and
Where Are We Now?***

Tuesday, February 11, 2020

I. Introduction

Mr. Chairman, Ranking Member, and Members of the Subcommittee, thank you for the opportunity to testify on “The Digital Millennium Copyright Act (DMCA) at 22: What it is, why it was enacted, and where are we now.” I am a professor at George Mason University’s Antonin Scalia Law School, where I run a legal clinic that provides pro bono services to individual artists and small businesses in the arts. My testimony today is informed largely by the experiences of such clients, though it is my understanding that concerns about the DMCA as interpreted by the courts and applied in practice are shared by the entire copyright sector. Regardless, I testify today only about my own views.

I will confine my comments to concerns about how Title II, and in particular, Section 512 of the DMCA has been applied in practice, because the community of creators I represent has not been particularly involved in the enforcement of Section 1201 of the DMCA, which addresses the circumvention of copyright protection systems. Their works are often distributed in formats which are not protected by Technological Protection Measures (TPMs), and to the extent they use formats protected by TPMs, they have benefitted from the efforts of corporate copyright holders to ensure the continued viability of those formats. Likewise, most of the creators with whom I work have not been hindered in achieving their creative vision by others’ use of TPMs.¹

It is worth noting that Section 1201 appears to have engendered continued voluntary cooperation between stakeholders across industry sectors, and litigation regarding the limits of Section 1201, such as *Lexmark*² and *Chamberlain Group*,³ has generally hewed to the expected contours of 1201. Unfortunately, this has not been the experience with Section 512. Section 1201 proceeds from the understanding that the use of TPMs allows all stakeholders to build new businesses and is thus drafted as an obligation to respect TPMs. In contrast, Section 512 imposes no direct obligations on any party, but rather

¹ Joseph Fishman, *Creating Around Copyright*, 128 HARV. L. REV. 1333, 1339 (2015); David Newhoff, *Fresh Scholarship on Copyright*, THE ILLUSION OF MORE (July 19, 2014), <https://illusionofmore.com/copyright-generative/>; see also David Newhoff, *Copyright and the Creative Process*, THE ILLUSION OF MORE (July 7, 2013), <https://illusionofmore.com/copyright-and-the-creative-process/>.

² *Lexmark Intern., Inc. v. Static Control Components, Inc.*, 572 U.S. 118 (2014).

³ *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004).

urges cooperation between stakeholders and grants service providers a conditional safe harbor. As a result, internet businesses are motivated to expand the intended application of safe harbors of Section 512, while limiting any conditions that may be placed on them. In this they have succeeded.

II. The Bargain Congress Expected in Enacting Section 512 Was Not Achieved

Congress enacted the DMCA in 1998 in order to address new challenges and opportunities presented by the Internet.⁴ Legislative history indicates that Congress intended to “preserve strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that occur in the digital networked environment.”⁵ Congress meant to establish an online environment where service providers can start new innovative businesses, while ensuring that infringing materials made available by users are rapidly removed or prevented from being made available in the first place.⁶

These twin goals were to be achieved through the provisions in Title II of the Act, which provide for certain safe harbors from liability for service providers if they:

- Designate an agent for receiving notices of infringement;
- Expeditiously remove infringing materials when notified by copyright owners, including if those notices are comprised of representative lists of infringing works;
- Implement repeat infringer policies; and
- Accommodate standard technical measures used to protect copyrighted works from infringement.⁷

Because Congress intended to preserve strong incentives created by case law for service providers to take an active role in preventing infringement on their networks, rather than turning a blind eye to obvious infringements, it also included a so-called “red flag” knowledge standard in Section 512.⁸

A. Red Flag Knowledge

Unfortunately, in the 22 years since the DMCA was passed, Section 512 has been misinterpreted by the courts in a way that has eviscerated the red flag knowledge standard and transformed Section 512 into a mere “notice and takedown” provision. Service providers have obtained the benefits of the safe harbors merely by responding to notices of infringement sent by copyright owners. Representative lists of infringements have gone by the wayside. Authors bear the entire burden of monitoring for and reporting infringements, and works are repeatedly reposted often moments after they are removed.

⁴ S. Rep. No. 105-190 at 1-2 (1998) (hereafter Senate).

⁵ H.R. Rep No. 105-551 at 49 (1998).

⁶ Senate at 21.

⁷ 17 U.S.C. § 512.

⁸ Senate at 40.

Because Section 512’s protections for copyright owners have been largely gutted by the courts and ignored by service providers, many see copyrighted works as assets free for the taking to spawn new internet businesses. Indeed, the situation is so dire that some internet entrepreneurs perversely refer to having a “DMCA license” (e.g. the right to use copyrighted works without permission until notified otherwise).⁹ This was not Congress’ intent.

A significant reason for the problems with Section 512 as applied is that service providers have no incentives to participate actively in ensuring their networks are free of infringing works. Although the Senate Report notes “Section 512 does not require use of the notice and takedown procedure,” instead, upon “obtain[ing] . . . knowledge or awareness” of infringing activity, the service provider must “act expeditiously to remove the material”¹⁰ in order to maintain the protections of the safe harbors. Unfortunately, courts have interpreted these provisions of the law, which ought to ensure active participation by service providers in limiting infringements, so narrowly as to make them meaningless.

Although Congress did not obligate service providers to actively seek out infringements, it did require them to act expeditiously to remove infringing materials once they have knowledge or awareness of infringing activity on their networks.¹¹ This knowledge or awareness may arise in two ways: actual knowledge that the specific material or an activity using the material on the system is infringing (actual knowledge),¹² or “awareness of facts or circumstances from which infringing activity is apparent (red flag knowledge).”¹³ In other words, actual knowledge is meant to be specific, and red flag knowledge requires merely a general awareness of infringement.¹⁴

The statutory requirement that Internet Service Providers (ISPs), search engines and websites respond to “red flag knowledge” that sites are infringing by refusing to index them, host them or by removing infringing materials has been all but nullified by the courts in a series of decisions in the Second and Ninth Circuits.

i. *Perfect 10, Inc. v. CCBill LLC*

In *Perfect 10, Inc. v. CCBill LLC*, the Ninth Circuit held that when a website referred to works it made available as illegal or stolen, red flag knowledge did not attach.¹⁵ This is flatly contrary to what the Senate said when enacting the bill. In fact, the Senate report used precisely such examples to explain when red flag knowledge applies. Speaking about the obligations of search engines it said “sites that are obviously infringing because

⁹ Corey Field, Esq., *The DMCA License?*, ASSOCIATION OF INDEPENDENT MUSIC PUBLISHERS (June 6, 2013), https://www.aimp.org/copyrightCorner/8/The_DMCA_License (last visited Feb. 10, 2020).

¹⁰ Senate at 44-45.

¹¹ Senate at 44.

¹² 17 U.S.C. § 512(c)(1)(a)(i).

¹³ 17 U.S.C. § 512(c)(1)(a)(ii).

¹⁴ Melville B. Nimmer & David Nimmer, *Nimmer on Copyright* § 12B.04(A)(1)(b)(ii) (“[T]o show that a red flag disqualifies a defendant from the safe harbor, the copyright owner must simply show that ‘infringing activity’ is apparent – pointedly, not *the* infringing activity.”).

¹⁵ *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007).

they . . . use words such as pirate, bootleg, or slang terms . . . to make their illegal purpose obvious . . . from even a brief and casual viewing” raise the red flag.¹⁶ Applying the Senate’s clear intent, one would have expected a different result in this case. Likewise, one would expect sites like The Pirate Bay would cease appearing in search results, however Google and other search engines continue to index and make available the millions of infringing files available there -even though they clearly have the technical knowhow to prevent these links from appearing in the results.

ii. *Viacom v YouTube*

In *Viacom v YouTube* the Second Circuit further eroded the meaning of red flag knowledge by limiting the obligations of defendants under the red flag knowledge standard to instances where they have knowledge of specific infringing activity.¹⁷ This collapses the distinction between actual and red flag knowledge.

iii. *UMG v. Shelter Capital*

In *UMG v. Shelter Capital* the Ninth Circuit adopted the reasoning in *Viacom*, and required specificity for red flag knowledge. Adding insult to injury, the court opined that requiring copyright owners to send takedown notices identifying specific instances of infringement would foster cooperation between copyright owners and service providers.¹⁸ This opinion not only did away with the distinctions between actual and red flag knowledge, but also ignored Congressional intent in separately defining notice and takedown requirements and requirements for service providers to take action when they develop actual or red flag knowledge on their own.

iv. *Capitol Records v. Vimeo*

Finally, in *Capitol Records v. Vimeo*, the Second Circuit held that the red flag knowledge standard was not triggered when employees of a service provider viewed entire, full length copies of currently popular copyrighted works on the service.¹⁹ According to the Second Circuit this could be decided as a matter of law on summary judgment – it was not for the jury to decide whether the viewed material was so obviously infringing as to raise a red flag.²⁰ Pointedly, this occurred in a case where discovery had revealed emails from managers to employees winkingly encouraging infringement (“we can’t officially tell you that using copyrighted music is OK, but . . .”). As one author put it:

Here’s where we are after *Capitol Records v. Vimeo*: A service provider can encourage its users to infringe on a massive scale, and so long as the infringement it encourages isn’t the specific infringement it gets sued for, it wins on the safe harbor defense at summary judgment. This is so even if there’s copious evidence

¹⁶ Senate at 48.

¹⁷ *Viacom Intern., Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012).

¹⁸ *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021-22 (9th Cir. 2013).

¹⁹ *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d. 78, 93 (2d Cir. 2016).

²⁰ *See id.*

that its employees viewed and interacted with the specific infringing material at issue. No jury will ever get to weigh all of the evidence and decide whether the infringement is obvious. At the same time, any proactive steps taken by the service provider will potentially open it up to liability for having actual knowledge, so the incentive is to do as little as possible to proactively “detect and deal” with piracy. This is not at all what Congress intended. It lets bad faith service providers trample the rights of copyright owners with impunity.²¹

B. Notice and Takedown

There is little evidence of shared responsibility in detecting and dealing with infringements with respect to other safe harbor conditions as well. The notice and takedown process itself is challenging, to say the least.

Testifying before the House of Representatives Judiciary Committee in 2014, GRAMMY winning composer/conductor/producer, Maria Schneider lamented

I come here as an independent musician in the prime of my career, grateful for a steadily growing fan base and critical acclaim. But my livelihood is being threatened by the illegal distribution of my work that I cannot reign in. . . . I’m now struggling against endless Internet sites offering my music illegally. After I released my most recent album *Winter Morning Walks*, I soon found it on numerous file sharing websites. Please understand, I am an independent artist and I put \$200,000 of my own savings on the line and years of work for this release, so you can imagine my devastation.

Taking my music down from these sites is a frustrating and depressing process. The DMCA makes it my responsibility to police the entire Internet on a daily basis. As fast as I take my music down, it reappears again on the same site – an endless whac-a-mole game.²²

Policing the internet for infringement is also becoming increasingly difficult and risky. During the fall semester of 2016, as part of my clinic’s study of the DMCA, students assumed the responsibility of enforcing copyright claims for a variety of artists and small businesses using the notice and takedown provisions of the DMCA.

Although the students had training in copyright law, and were coached on the DMCA process by experts, they still found the effort confusing and frustrating. Search results often returned a high number of possible infringements. Clicking through the results was not only time consuming, but often led them to phishing and other malicious sites. Once infringement was found, searching websites and ISP directories to identify the proper DMCA agent to notify was often difficult or futile. Effective notice sending was thwarted

²¹ Devlin Hartline, *Capitol Records v. Vimeo: Courts Should Stop Coddling Bad Actors in Copyright Cases*, IP WATCHDOG (June 22, 2016), <https://www.ipwatchdog.com/2016/06/22/capitol-records-vimeo-copyright/id=70288/>.

²² H.R. Rep. No. 113-86, at 57 (2014).

by non-uniform forms that were challenging to find and complete accurately. After having devoted numerous hours to these tasks the students often received no response. On other occasions, students were asked to justify their requests and to provide information or proof beyond what the statute requires before their notices were honored.

Language on some sites regarding when a notice may be sent was intimidating, and would be even more so for an artist without legal training. Students were also constantly dealing with IT problems as a result of visits to untrustworthy sites.

Sadly, all of these challenges persist despite multiple studies, hearings and roundtables organized by the United States Copyright Office, United States Patent and Trademark Office, and the National Telecommunications and Information Administration, to urge collaboration between ISPs and copyright owners and reform of current practices.

There is a disconnect in how the creative community and the internet community view the operation of the DMCA. Artists and their representatives have cautioned that without shared responsibility the situation for creative expression on the internet will continue to deteriorate. Meanwhile, internet entrepreneurs who profit from infringing works on their services believe that the DMCA is serving its purpose. Instead of identifying means of better cooperation to achieve all of the stated goals of the DMCA, internet companies speak primarily of the unanticipated consequences of non-compliant notice sending. They apparently do not recognize that the percentage of noncompliant notices is vanishingly small when compared to the tsunami of notices copyright owners must send daily.

In 2014 several professors affiliated with “the Takedown Project” – a group of researchers concerned about the effect of take down notices on freedom of speech – sought evidence to demonstrate that internet users’ speech is harmed when take down notices are sent improperly.²³ The researchers manually reviewed 3,500 notices to find evidence of mistakes or misdirection. Having found mistakes in approximately 1/3 of the notices reviewed, the researchers suggest a variety of policy reforms to make the sending of takedown notices less likely, and to impose stronger penalties on notice senders who make mistakes or send improper notices.²⁴ Although the task of reviewing the thousands of notices selected by the project is certainly impressive, the results do not support the group’s proposed reforms. Economist George York explains:

“Everyday Practice” is a herculean research effort but, as I detail herein, the empirical analysis in “Everyday Practice” cannot justify its policy recommendations. To begin, the data analyzed in Everyday Practice are non-randomly selected and nonrepresentative of the world of notice and takedown.

²³ Jennifer M. Urban et. al., *Notice and Takedown: Online Service Provider and Rightsholder Accounts of Everyday Practice*, 64 COPYRIGHT SOC’Y U.S.A. 371 (2017) (hereafter “Everyday Practice”); see also D. Seng, *The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices*, 18 VA. J.L. & TECH. 369, 473 (2014), http://www.vjolt.net/vol18/issue3/v18i3_2Seng.pdf.

²⁴ If internet advocates are concerned about improper takedown notices, a better solution is to enact the Copyright Alternative in Small-Claims Enforcement Act of 2019 (CASE Act), S.1273, which would allow individuals harmed by such notices to pursue claims against copyright owners who sent them in a small claims forum established within the Copyright Office.

The authors of the study admit their empirics cannot be extrapolated to the entire world of notice sending but they do exactly that, thereby committing the original sin of empirical analysis. Perhaps more fatal than the data concerns, however, is that while recognizing that the benefits of a policy change must exceed its costs, the authors never quantify, even loosely, the costs or the benefits of their proposals. In fact, while the study appears motivated by speech concerns, Everyday Practice fails to quantify the incidence of takedowns impinging on legally protected speech and offers no evidence that the alleged “questionable notices” are of the sort that impact speech or cause any harm at all (other than to rightsholders). Indeed, the authors describe most of the problems as “minor sins of misidentification,” and they are unable to determine whether harmful requests actually lead to takedowns. Google, for its part, indicates that it will “push back on these requests when they fail to include the necessary information or we suspect they are fraudulent.” A mistaken request that is not acted upon causes no harm to expression. Without any demonstrated harm to online expression, there is no basis for the policy reforms of the sort Everyday Practice sets forth.²⁵

C. Repeat Infringer Policies

Recently corporate copyright owners have had some success litigating against ISPs who fail to enforce their own publicly announced repeat infringer policies, but this can hardly be considered a victory. The fact patterns in these cases are so beyond the pale that they have inspired amusing headlines not just in trade journals, but in the daily press. *Fourteen Strikes And You’re Out. Or Not. Emails Reveal How Cox Lost The Safe Harbor* quipped the UK broadsheet *The Register*.²⁶ And *Digital Music News* chose to quote one of the Cox emails as its headline: *Cox Executive Declares: F*** the DMCA!!!*²⁷

As the headlines suggest, in *BMG v. Cox*, Cox failed to enforce even its own, utterly toothless repeat infringer policy. Cox customers were afforded thirteen “strikes” or notices that they had uploaded infringing works before being terminated.²⁸ However, as soon as they were terminated customers could open a new account and reset the infringement count to zero.²⁹ Emails found during discovery revealed the disdain in which Cox executives held copyright law.³⁰ Not surprising, the customers Cox sought to

²⁵ George S. Ford, *Notice and Takedown in Everyday Practice: A Review* at 2, (April 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2963230#.

²⁶ Andrew Orłowski, *14 Strikes and You’re Out. Or Not. Emails Reveal How Cox Lost Safe Harbor*, THE REGISTER (Dec. 3, 2015), https://www.theregister.co.uk/2015/12/03/14_strikes_out_internal_emails_reveal_how_cox_lost_safe_harbor/.

²⁷ Paul Resnikoff, *Cox Communications Executive Declares: “F*** the DMCA!!!*”, DIGITAL MEDIA NEWS (Dec. 15, 2015), <https://www.digitalmusicnews.com/2015/12/15/coxs-manager-of-abuse-operations-declares-fuck-the-dmca/>.

²⁸ *BMG Rights Management (US) LLC. v. Cox Communications, Incorporated*, 881 F.3d 293, 299 (4th Cir. 2018).

²⁹ *Id.* at 303.

³⁰ *See id.*

retain by failing to enforce its own policies were some of its better paying customers who desired high speed service in order to make infringement more convenient.³¹

I was disappointed that various parties weighed in with amicus briefs arguing that takedown policies could not be applied if more than one user in a household used the internet service. Apparently these parties believe high speed internet service is more of a basic human necessity than housing or transportation, which can both be seized under federal forfeiture laws regardless if jointly held. While I do not suggest that the circumstances under which federal forfeiture is permitted are exactly comparable, surely if the seizure of a jointly owned home or automobile is permissible, disabling internet service must also be under appropriate circumstances. Clearly ISPs have no qualms disabling service for nonpayment, for instance.

IP skeptics and groups like Electronic Frontier Foundation and Public Knowledge likewise argued that the repeat infringer policies should apply only to parties who have repeatedly been adjudicated in federal court as infringers.³² Setting aside for the moment that individual artists and small businesses are not able to afford to bring a single federal lawsuit, much less fourteen, these skeptics must be congratulated on their ability to keep a poker face while suggesting that such an interpretation of the law could be in line with the DMCA's stated goal of providing a streamlined means of protecting copyrighted works on the internet.

D. Similarities with Section 230 of the Communications Decency Act

The disappointments of Section 512 of the DMCA are not unique. Indeed, Section 512 was enacted on the heels of the Communications Decency Act, (CDA) passed two years earlier. Section 230 of the CDA provides a limitation on liability for online platforms, websites and internet service providers for materials provided by third parties. Court decisions and common practice have evolved to allow such immunity regardless of how vile, illegal, dangerous or threatening the third-party posting is. It is often pointed out that Section 230 consists of only 26 words, but that those words are credited with “launching the internet.”³³ Section 230 stipulates:

“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”³⁴

The CDA did not address liability for copyright infringement, thus setting the stage for negotiations on protections for internet businesses in the context of the DMCA.

³¹ Compl. ¶ 19, *BMG Rights Management (US) LLC. v. Cox Communications, Incorporated*, 2014 WL 11030947.

³² Amicus Curiae Brief of United States Telecom Association in Support of Defendants-Appellants, *BMG Rights Management (US) LLC. v. Cox Communications, Incorporated*, 2014 WL 11030947 at *12 (quoting Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1420-21 n. 130 (2004).).

³³ See Jeff Kosslef, *The Twenty-Six Words that Created the Internet* (2018).

³⁴ 47 U.S.C. § 230.

Much like the experience with Section 512 of the DMCA, Section 230 of the CDA has provided online services what amounts to complete immunity for materials posted by users on their portals. In recent years it has become clear that the very broad interpretation of Section 230 is allowing services to benefit from user posting of illicit materials ranging from child pornography to revenge porn and human trafficking. Notably, almost all of the user postings related to these activities consist of paid advertising on platforms like Craig’s List and Backpage.

Authors and supporters of the original CDA have expressed genuine dismay that the protections enacted in Section 230 intended to foster the flowering of dialogue, free speech and online communities have instead become shields to allow internet sites to profit from the sale of advertising for illegal activities. In a recent interview with Pro Market, the University of Chicago Business School’s blog former FCC Chairman Reed Hunt said,

We were naïve. We were naïve in a way that is even hard to recapture. We all thought that for people to be able to publish what they want would so enhance democracy and so inspire humanity, that it would lead to kind of flowering of creativity and emergence of a kind of a collective discovery of truth.³⁵

In an attempt to roll back some of the most damaging expansions of Section 230, Congress passed legislation in 2018 to allow states and victims to fight online sex trafficking.³⁶ The Act was needed because

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) section 230 of the Communications Act of 1934 (47 U.S.C. 230; commonly known as the “Communications Decency Act of 1996”) was never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims;

(2) websites that promote and facilitate prostitution have been reckless in allowing the sale of sex trafficking victims and have done nothing to prevent the trafficking of children and victims of force, fraud, and coercion; and

³⁵ Guy Rolnik and Eytan Avriel, “*We Were Naïve,*” Says FCC Chair Who Oversaw the Creation of Section 230, PROMARKET (Jan. 23, 2020), <https://promarket.org/we-were-naive-says-the-fcc-chair-who-oversaw-the-creation-of-section-230/>.

³⁶ Fight Online Sex Trafficking Act of 2017 (FOSTA), H.R. 1865, P.L. No. 115-164, 115th Congress (2017-2018); Stop Enabling Sex Traffickers Act of 2017 (SESTA), S. 1693, 115th Congress (2017-2018).

(3) clarification of such section is warranted to ensure that such section does not provide such protection to such websites.³⁷

Although the carve outs from Section 230 in the bills were extremely limited, and applied only to websites that promote and facilitate prostitution by advertising the sale of unlawful sex acts, it too spawned outcry from advocates for internet companies, who mounted fundraising campaigns on the basis that they “not only fought the bill in Congress, but when the President signed it into law, set our sights on challenging it in courts.”³⁸

I address Section 230 for two reasons. First, because it illustrates that the protections we believed necessary for the growth and development of the internet more than 20 years ago, have not withstood the test of time, and have instead brought unintended consequences. Also, because the Section 230 experience demonstrates that targeted changes to reset provisions which have served the development of the internet well are possible without dire consequences. In the case of changes to Section 230, it is notable that the offending services discontinued the advertising complained of without the need for litigation by states and victims. This suggests that even conducting these hearings and fleshing out the scope of any contemplated legislation to rebalance the operation of the DMCA can have a salutary effect.

III. Conclusion

On behalf of independent artists and small businesses, who do not have the wherewithal to continue futile enforcement efforts under the current circumstances, I thank you for your interest in holding hearings aimed at introducing legislation to remedy the problems identified. The goal of any legislation should be to develop solutions in tune with not just today’s, but the next generation’s internet. The DMCA was passed almost a generation ago when the internet companies that benefit from its (and Section 230’s) safe harbors either did not exist yet, or were in their infancy. Now they are major multi billion dollar companies that wield outside impact on virtually every aspect of our lives.

I do not advocate doing away with the protections safe harbors have afforded internet companies, because along with the negative, they have also done much to spur positive developments and creativity on the internet. Nevertheless, I believe that the last twenty-two years of applying the DMCA to everyday practice have demonstrated that the marketplace and the courts have eroded the original intent of Congress. In considering legislation, it will be important to focus on how best to restore those elements of the DMCA intended to foster cooperation between stakeholders. One clear area of legislative reform would be to restore/clarify the original meaning of red flag knowledge. Similarly, elements of the DMCA which have received little or no attention -- such as the concept of

³⁷ 47 U.S.C. § 230 (2018).

³⁸ Aaron Mackey & Elliot Harmon, *Congress Censors the Internet, But EFF Continues to Fight FOSTA: 2018 in Review*, ELECTRONIC FRONTIER FOUNDATION (Dec. 29, 2018), <https://www.eff.org/deeplinks/2018/12/congress-censors-internet-eff-continues-fight-fosta-2018-review>.

sending notice of infringements by means of representative lists, rather than link by link, and the requirement to accommodate standard technical measures, should be revisited and incorporated more effectively into any new legislation. Much has also been said about the concept of “notice and staydown”, and I certainly support that goal. Legislation could provide incentives for internet businesses to incorporate technologies or policies to bring us closer to that goal. Some progress has already been made on this in the European Union Digital Single Market Directive, demonstrating not only that this is an achievable goal, but that internet services operating in the EU will already be required to meet such standards.³⁹

There are also practical measures stakeholders could pursue independently of legislation such as creating a uniform, automated means of providing notices, allowing all copyright owners access to technology and tools such as the technology behind Content ID that make monitoring and sending of notices more efficient, and enumerating technologies which have become “standard” to screen works prior to upload, or to make identification and removal or monetization of infringing posts easier.

I thank you for your attention to these important matters, and for the opportunity to share my thoughts.

³⁹ Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, 2019 OJ (L 130/92), <https://eur-lex.europa.eu/eli/dir/2019/790/oj>.